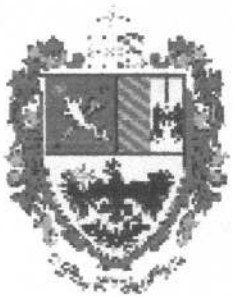
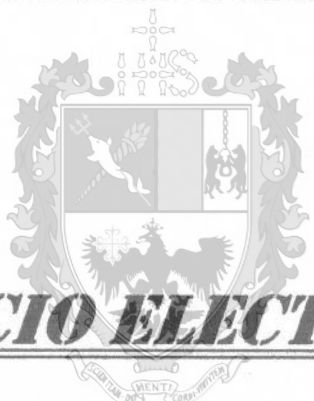


UNIVERSIDAD DEL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

TESINA FINAL



"COMERCIO ELECTRÓNICO"

Profesor Tutor: Dr. Roberto De Simone

Autor: María Eugenia Belgrano

"...Históricamente el mercado fue el lugar donde los caminos y los ríos se cruzaban, donde los comerciantes y caravanas hacían un alto en el recorrido, donde los agricultores llevaban sus productos y los artesanos sus habilidades. En la nueva economía ya no es así... vemos un cambio de una extraordinaria importancia histórica y sociológica: el cambio en la naturaleza de los mercados de lugares a redes..." (BELL, Daniel. *"El mundo en 2013"*, en Facetas 3, 1988)

- **ÍNDICE**

INTRODUCCIÓN

El crecimiento del comercio electrónico está siendo tan grande que prácticamente nadie duda del profundo impacto económico y social que está produciendo, y todos los actores involucrados, desde gobiernos a asociaciones de la industria y empresas individuales, tratan de tomar las medidas necesarias para aprovechar al máximo sus ventajas.

El comercio electrónico:

- Permite hacer más eficientes las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales, en especial para pequeñas empresas, y abre oportunidades de explotar mercados nuevos.
- Para el consumidor, amplía su capacidad de acceder a prácticamente cualquier producto y de comparar ofertas, permitiéndole además convertirse en proveedor de información.
- Reduce o incluso elimina por completo los intermediarios, por ejemplo en la venta de productos en soporte electrónico (textos, imágenes, vídeos, música, programas, etc.) que se pagan y entregan directamente a través de la red.

Pero el comercio electrónico plantea también problemas nuevos o agudiza algunos ya existentes en el comercio tradicional, entre ellos:

- La validez legal de las transacciones y contratos "sin papel"
- La necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio
- El control de las transacciones internacionales, incluido el cobro de impuestos
- La protección de los derechos de propiedad intelectual
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales
- La dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica
- La seguridad de las transacciones y medios de pago electrónicos

Ya es cada vez más notorio como la tecnología va avanzando con el pasar del tiempo y en especial la llamada Internet, que permite comunicarse con todo el mundo a bajo costo y con gran rapidez.

Es así que esto permitió el surgimiento de la firma digital como un modo de dar seguridad a los actos que se celebran a través de la Red. En consecuencia fue válido fomentar el desarrollo del comercio electrónico.

El presente trabajo apunta a mostrar las herramientas que hacen posible el comercio electrónico, y cuáles son las dificultades que presenta desde el punto de vista impositivo, en cuanto a la protección del consumidor y sobre la celebración de contratos por Internet, tratando de adecuar lo tradicional a lo virtual, con la ayuda de normas para fundamentar el apogeo del comercio electrónico; apunta a analizar las desventajas enumeradas precedentemente.

CAPÍTULO I

"Seguridad en las transacciones electrónicas"

Firma digital

Tanto la seguridad como la privacidad son relevantes a la hora de pensar en un crecimiento del comercio electrónico, teniendo en cuenta que el mismo permite agilizar las operaciones como también ahorrar costos y tiempo.
Estos dos conceptos se ven afectados por lo siguiente:

La autenticidad en cuanto al origen del emisor del mensaje
La integridad en cuanto al contenido original del mensaje, ya que el mismo puede ser alterado durante el transcurso del emisor al receptor
El "no repudio" del mensaje emitido que significa que quien emitió el mensaje no puede negar que lo hizo
La confidencialidad del mensaje

Para solucionar esto aparece la firma digital que es el resultado de una transformación de un documento digital empleando un criptograma asimétrico (que es un algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar esa firma digital, el que deber ser técnicamente confiable, es decir que cumplan con los estándares tecnológicos que al efecto dicte la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros) y un digesto seguro (que es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada de esa manera, de forma tal que se obtenga la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital, y de esta manera es computacionalmente no factible inferir o reconstruir un documentos digital a partir de su digesto seguro, como así también tampoco es factible encontrar dos documentos digitales diferentes que produzcan el mismo digesto seguro). Así una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar:

- Que la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante;

- Si el documento digital ha sido cambiado desde que se realizó la transformación.

El conjunto de estos dos requisitos precedentes garantiza su no repudio, es decir la cualidad de la firma digital, por la cual el autor no puede desconocer un documento digital que el ha firmado digitalmente; y su integridad, o sea la condición de no alteración de un documento digital.

De acuerdo a la reglamentación de la ley 25.506 (ley de firma digital) existen sistemas de comprobación de estas dos condiciones:

1) Firma electrónica, la que se considera con carencia de algunos de los requisitos legales respecto de la firma digital; quien la utiliza es quien debe satisfacer su validez (en cambio en la firma digital, la validez de la misma la garantiza un certificador licenciado, que vincula los datos de verificación de firma a su titular).
2) Firma digital respecto de certificados emitidos por:
   a. Certificadores no licenciados
   b. Certificadores licenciados.
   c. Certificadores extranjeros, siempre que reúnan los requisitos establecidos para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la Argentina y el país de origen del certificador extranjero; o los certificados hayan sido reconocidos por un certificador licenciado en el país, cuyo reconocimiento deberá ser validado por la autoridad de aplicación, o sea la Jefatura de Gabinete de Ministros (según lo establece el art. 29 de la ley 25506).

Vale decir respecto del punto 2) a. que los mismos serán válidos para producir los efectos jurídicos establecidos para la firma electrónica. Es por esto que a partir del decreto 724/2006 se establece firma *electrónica* respecto de certificados emitidos por certificadores no licenciados.

En el mundo de la escritura y el papel, es posible realizar una comparación entre el documento original y el falso para deducir la autenticidad; es factible la prueba empírica respecto de la firma consignada en el documento; se puede tomar un papel, analizarlo, someterlo a dictámenes, hacer pericias caligráficas sobre una nueva escritura comparativa del firmante, en cambio en el mundo virtual no es posible la prueba empírica comparativa, el documento original puede ser igual que el falso, porque no hay bits falsos; un bit hará una copia exacta de otro bit original (LORENZETTI: 2001, 59).

Procedimiento para garantizar "el secreto" de la transacción realizada:

En primer lugar se debe crear el texto del mensaje a enviar; luego hay que conocer la clave pública del receptor (la cual puede ser obtenida a través del requerimiento de la misma al emisor, porque la obtuvo de la web, por listados publicados de direcciones electrónicas, entre otras). Mediante la utilización de la clave pública se procede a encriptar el mensaje y luego el receptor mediante su clave privada lo desencripta.

Cabe señalar que la clave pública posee exclusivamente una clave privada que es su par, por lo que resulta imposible que la misma sea descubierta o descifrada, salvo que su propietario la de a conocer a terceros.

Cabe destacar que una vez encriptado el mensaje sin haber sido enviado al receptor, si el emisor quiere modificar algo en el mismo, la única alternativa que tiene es borrarlo y volver a preparar uno nuevo correctamente. Para el receptor es importante reconocer la autenticidad de la identidad del emisor del mensaje, porque como la clave pública es de amplio conocimiento, existe el riesgo que por algún motivo un tercero quiera representar al emisor, es por esto necesario que el emisor atache al mensaje su firma digital, para su encriptación el emisor utiliza su clave privada para que de esta forma el receptor pueda verificar la autenticidad de la firma del emisor utilizando su clave pública procediendo a desencriptar la clave privada constatando la identidad del mismo.

La firma digital requiere la certificación de una autoridad para verificar la identidad del firmante digital controlando las claves públicas y privadas de encriptación.

Es muy común que, mientras un vendedor y un comprador pueden estar interesados en una espléndida transacción comercial, ninguno de los dos confía en el otro, por lo tanto el rol de la autoridad certificante que certifica la identidad de las partes intervinientes en la operatoria es de gran utilidad para el comprador como el vendedor (NUÑEZ: 2001, 58).

Los certificadores licenciados son los encargados de emitir los certificados a los suscriptores, y para obtener la licencia deben especificar las actividades por las cuales quieren la misma, acreditando documentación que demuestre:

Si se trata de personas jurídicas, su personería, en el caso de registro público de contratos, tal condición. Si es una organización pública, deben estar autorizadas por su máxima autoridad para licenciarse, como también la aprobación de la Jefatura de Gabinete de Ministros. Las entidades que controlan la matrícula, en relación a la

prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma escrita, cumpliendo con los requisitos para ser certificador licenciado.

Tendrán que establecer las políticas de certificación para las cuales piden licencia que respalden la emisión de sus certificados: Manual de Procedimientos, **Plan de Seguridad**, Plan de Cese de Actividades y Plan de Contingencia. Estas políticas deben contener como mínimo la identificación del certificador licenciado, política de administración de los certificados y detalles de los servicios arancelados, obligaciones de la entidad y de los titulares de los certificados, como así también el tratamiento o verificación de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso; y garantías que ofrece respecto del cumplimiento de las obligaciones que provengan de sus actividades.

Tienen que estar predispuestos a dar toda aquella información que requiera la Autoridad de Aplicación.

La licencia dura 5 años y pueden ser renovadas y cada año deben presentar una Declaración Jurada que demuestre que han cumplido con las normas de firma digital, vale decir en este caso que serán sometidos a auditorías anuales.

Escribano o cibernotario

El certificado de clave pùblica es otorgado por el certificador y relaciona la clave pùblica con su suscriptor. Cuando actúa un escribano, las autoridades certificantes delegan la recepción de la solicitud y la consecuente identificación del interesado en las autoridades de registro, el cibernotary (escribano o cibernotario) tiene la función de realizar una investigación de los usuarios que deseen registrar sus claves públicas para utilizarlas en el comercio electrónico. Puede existir una certificación de bajo valor, donde se establece la identidad del usuario para asignarle una clave pública, o una de alto valor donde el notario realiza una investigación sobre la historia crediticia y criminal del usuario antes que la clave sea emitida.

El notario funciona como una compuerta de seguridad para la entrada al e-commerce.

Por otra parte el suscriptor del certificado digital tiene las siguientes obligaciones:

- ❖ Proveer todos los datos requeridos por la autoridad certificante licenciada por el organismo licenciante bajo declaración jurada.
- ❖ Mantener el control de la clave privada e impedir su divulgación
- ❖ En caso de cualquier circunstancia que pueda haber comprometido su clave privada, informar inmediatamente a la autoridad certificante licenciada, así como también informar cuando cambie alguno de los datos contenidos en el certificado.

Validez del certificado de clave pública

a) Cuando es emitido por una autoridad certificante licenciada
b) No ha sido revocado
b) No ha expirado

Los certificados son utilizados para bloquear intentos de sustituir una clave por otra.
La principal función del certificado es asociar la identidad de una persona determinada a una clave pública específica (e,indirectamente, a una clave privada) (LORENZETTI: 2001, 85)

Un certificado de clave pública contiene los siguientes campos:

VERSION: identifica el formato del certificado
Nro. DE SERIE: Nro.de serie único
IDENTIFICADOR DEL ALGORITMO: identifica el algoritmo usado para firmar el certificado, junto con los parámetros necesarios
AUTORIDAD CERTIFICANTE LICENCIADA: su nombre
PERÍODO DE VALIDEZ: fecha de inicio y término de la validez del certificado
USUARIO: su nombre
CLAVE PÚBLICA DE USUARIO: incluye el nombre del algoritmo y parámetros necesarios
FIRMA: de la autoridad certificante licenciada

El formato debe responder a estándares reconocidos internacionalmente, fijados por la autoridad de aplicación y deben observarse los datos especificados precedentemente, ser